Qoria

11 Feb 2025

Strategic Market Status Investigations into Apple's and Google's mobile ecosystems: CMA's invitation to comment

By email: mobilesms@cma.gov.uk

We are pleased to have the opportunity to provide a response in relation to the CMA's invitation to comment on its SMS investigations into Apple's and Google's mobile ecosystems.

Key comments

Comment 1: *We urge immediate prioritisation of competition in safety technology.*

Children are exposed to worrisome online content and services from a vast array of sources. The community is clearly concerned with regulatory and media interest exploding.

Safety regulators are focussing on the major social media platforms for "reform" and considering or imposing platform gates eg age verification & parent consent.

In our considered view the objectives of these measures will fail without concurrent consideration of competition in safety technology. This is because:

- Proposed platform based / centralised gating modalities are extraordinarily problematic. Age verification and parent consent are readily bypassable. Age verification requires all adults to be identified to access the internet. And a focus on major platforms will move kids to more risky areas of the internet
- Given the breadth of the internet that kids access and increasing encryption, on-device (operating system level) safety is fundamental to directing kids to the safe & governable internet. App stores can't do this. Operating system capability however is tightly controlled by Google, Apple and Microsoft.
- Kids use many devices and online platforms, so requiring parents to set rules for each online platform and on each device they use is impractical.

The internet is so dynamic that prescriptive regulatory models cannot hope to keep up and Qoria therefore welcomes the CMA's Invitation to Comment and its broad consideration of the issues, which should allow the CMA to adapt to rapidly changing sectors and practices.

Interoperability-enabled competition in online safety is the only sustainable way to drive innovation and protect our kids.

Providers of safety technology require access to the mobile ecosystem in order both to access customers and for customers to be able to use the technology in the way in which they wish to do so. There, however, exists an inherent conflict of interest for platforms to ensure digital safety. While platforms may show support for the need to ensure digital safety because of its political momentum and the generalization of the concern among regulators, it should be recognised that effectively ensuring digital safety (in particular, for children) directly impacts on the user experience and on the subsequent acquisition of potential lifetime users. Given this inherent conflict, and the importance of digital safety to our society, the issues being faced by providers of safety technology should be examined when the CMA is considering any potential interventions, either through conduct requirements or pro-competition interventions.

For example, in relation to safety tech, Google and Apple's interest in maintaining their user experience and encouraging user acquisition/loyalty described above might mean that they may not only make third party apps that compete with their apps less discoverable, but may also provide less functionality to third party apps on personal devices when compared to greater functionality given to apps for business users, given Google and Apple's power over the mobile ecosystems on personal devices. This type of practice is not currently considered in the Invitation to Comment.

Comment 2: *We urge extension of 'ecosystems' with the explicit inclusion of remote management tools and user authentication.*

To deploy and manage 3rd party technology on Google and Apple platforms a range of Google and Apple technologies and services are interacted with.

Google and Apple's market power is exerted through this entire 'stack' which includes app market places, operating systems (including remote administration of operating systems), hardware (smart phones, tablets, glasses, gaming consoles), browsers, user authentication, financial transactions and now increasingly embedded AI capabilities.

For your consideration, we provide in the chart below a high-level overview of the components of a device ecosystem.

Cloud services & tools	Cloud management tools allow app developers (mostly enterprise) to deploy and manage their apps, extensions and profiles.
Browsers	**Apple:** Safari **Google:** Chrome **Microsoft:** Edge
Extensions	Extensions can be installed in and run in the browser to perform specific functions. This may be authentication, web filtering, and app user interfaces.
1st party apps & applications	**Apple:** App Store, iMessage, Facetime, Screentime, Apple Pay **Google:** Google Play, Family Link, Workspace, Google Pay **Microsoft:** Microsoft Family, Microsoft Office
Operating systems	**Apple:** iOS, MacOS **Google:** Android, Chrome OS **Microsoft:** Windows
Profiles & extensions	Can be installed in a run in the Operating System. They access features of the operating system that support functions like filtering, authentication & location.
Devices	**Apple:** iPads, iPhones, MacBooks, AirTag, Apple Watch **Google:** Android Devices, Chromebooks, Nest **Microsoft:** PCs, XBox

Using competition in safety technology as an example. For safety technology to compete with Google and Apple it must have fair, open, non-discriminatory access to:

- **App market places** so that the safety technology is discoverable;
- **Device onboarding wizards** so that consumers are aware that 3rd party options are available and so that impediments aren't applied to installing competing safety products;
- On-device **user management & authentication**, so safety tech can align with users set up by the parents across all device platforms;
- All **operating system features** and **device capabilities** to ensure the safety tech is installed reliably, can't be removed and can access the highest capability of the device in terms of location services, battery management and administrative functions such as controlling use of cellular services, VPNs, WiFi access, app access, messaging services etc;
- All **cloud management tools**, such as Apple Mobile Device Management and Google's Workspace tools so that technology can be seamlessly and reliably installed and managed; and
- All **browser capabilities** because this is where content filtering is best embedded so it can inspect content before encryption.

We note that under the CMA's Google Investigation Notice Native App Distribution is defined as a "service which enables the installation, distribution and operation of native apps on mobile devices, which are apps written to run on the Mobile Operating System". Whilst this prima facie would cover the cloud management tools app developers must use to deploy and manage their apps, we urge these tools be explicitly included in the ecosystem definition. For example, Figure 1.2 of the CMA's Invitation to Comment does not include all of these critical components

and when describing "native app distribution" in the Invitation to Comment, this states that the CMA's investigations will cover "Apple's and Google's distribution of apps through their respective app stores", which suggests that the CMA may be taking a narrower approach.

Without considering the entire "stack" as described in this submission, the CMA's investigations and subsequent actions may be ineffective due to Google and Apple's control over the entire stack and the corresponding ability to adapt business practices across the entire stack. The CMA should consider the digital activities holistically, irrespective of whether it decides to consider the digital activities as part of a grouped designation or as individual digital activities (and indeed should select the most appropriate designation to allow it to do so).

Effective and interoperability-enabled competition is the only means of ensuring digital safety precisely because of (i) the highly dynamic nature of digital ecosystems; and (ii) the inherent conflict of interest that gatekeepers/ecosystems may have in ensuring digital safety when it conflicts with user experience.

We would be happy to discuss these issues with the CMA in more detail, should that be helpful.

[redacted]

About Qoria

Qoria was founded (as Family Zone) in 2016 by four fathers following harrowing family experiences and deep concerns that tech was blinding parents and school device programmes were being thrust upon unprepared families.

Today we are known as Qoria, and we operate as Smoothwall in K12 and Qustodio in parental controls in the UK.

We develop and implement technology solutions and programs to promote the safe use of technology by children in schools and homes. We operate globally and now support 6 million parents and 27 thousand schools in their efforts to maintain online safety for 24 million children.

Our approach emphasises collaboration among school staff, teachers, and parents to make informed decisions about children's online activities.

To be clear, we are not advocating for our products or any products or providers. On the contrary, we advocate for policies that will be effective and will support competition, choice and proper regulatory oversight.